Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore Maya (SBN 223242)
tmaya@ahdootwolfson.com
Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
Christopher E. Stiner (SBN 276033)
cstiner@ahdootwolfson.com
Rachel Johnson (SBN 331351)
rjohnson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
Joseph W. Cotchett (SBN 36324)
jcotchett@cpmlegal.com
Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
Noorjahan Rahman (SBN 330572)
nrahman@cpmlegal.com
Julia Peng (SBN 318396)
jpeng@cpmlegal.com
COTCHETT, PITRE & McCARTHY LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: 650.697.6000
Facsimile: 650.697.0577

Interim Co-Lead Class Counsel
Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: ZOOM VIDEO COMMUNICATIONS, INC. PRIVACY LITIGATION	Case No. 5:20-CV-02155-LHK
This Document Relates To: All Actions	**CONSOLIDATED AMENDED CLASS ACTION COMPLAINT**
	DEMAND FOR JURY TRIAL

Plaintiffs Caitlin Brice, Heddi N. Cundle, Isabelle Gmerek, Cynthia Gormezano, Kristen Hartmann, M.F. and his parent Therese Jimenez, Lisa T. Johnston, Oak Life Church, Saint Paulus Lutheran Church and Stacey Simins ("Plaintiffs") allege the following against Defendant Zoom Video Communications, Inc. ("Defendant" or "Zoom"), acting individually and on behalf of all others similarly situated:

BRIEF SUMMARY OF THE CASE

1. Plaintiffs bring this case to stop Zoom, currently the most popular videoconferencing platform, from invading consumers' privacy and from promoting its product under false assurances of privacy. Further, Plaintiffs seek compensation for themselves and all others similarly situated for past privacy violations.

2. Zoom is a supplier of video conferencing services founded in 2011 by Eric Yuan, a former corporate vice president for Cisco Webex. In January 2017, Zoom raised $100 million in Series D funding from Sequoia Capital at a $1 billion valuation, and achieved "unicorn" status—a privately held startup that has reached a $1 billion valuation. On April 18, 2019, the company became a public company via an initial public offering. On its first day of trading Zoom's share price increased over 72%, and by the end of the day Zoom was valued at $16 billion. By June 2020, Zoom was valued at over $67 billion.

3. Zoom achieved this remarkable growth by, as explained by Mr. Yuan, taking "the work out of meetings." "We've dedicated ourselves to the features and enhancements that pull all the friction out of video communications. We've made it easier to buy and deploy Zoom Rooms, we've made it simpler to schedule meetings and manage rooms."[1] What was not explained, and what has become evident since Zoom's widespread adoption, is that Zoom's focus on its goal of "frictionless" video conferencing came at the cost of proper attention being placed on security and on ensuring that Zoom users' private moments would not be shared with, exploited by, or obscenely hijacked by others.

[1] Priscilla Barolo, *Zoom Launches Enhanced Product Suite to Deliver Frictionless Communications* (Jan. 3, 2018), available at <https://blog.zoom.us/zoom-launches-enhanced-product-suite-to-deliver-frictionless-communications/> (Last Visited July 28, 2020).

4. In early 2020, usage of video conferencing, especially Zoom, increased dramatically in response to the COVID-19 pandemic. As of the end of December 2019, the maximum number of daily meeting participants, both free and paid, conducted on Zoom was approximately 10 million. In March 2020, Zoom reached more than 200 million daily meeting participants, both free and paid.[2] With the surge in usage also came increased scrutiny on Zoom's privacy policies and new flaws were revealed almost on a daily basis.[3]

5. On March 26, 2020, an article on Vice News' Motherboard tech blog revealed that, unbeknownst to users, the Zoom iPhone app was sending users' personal data to Facebook even if users did not have a Facebook account.[4] Zoom was providing a trove of data to third parties through its Apple iOS app, which implemented Facebook's user login "Software Development Kit" (SDK). Zoom admitted that it permitted the Facebook SDK to collect and share user information including: device carrier, iOS Advertiser ID, iOS Device CPU Cores, iOS Device Display Dimension, iOS Device Model, iOS Language, iOS Time zone, iOS Version.[5] While Zoom reported to have removed the Facebook SDK, Zoom continues to share similarly valuable user data with Google via that company's Firebase Analytics. Plaintiffs never granted permission for third parties to extract and use such data—indeed, they were not even aware of the data transmission.

6. First and foremost this collection and sharing of Plaintiffs' data presented an egregious invasion of their privacy. As well, surreptitious transfer of data by Zoom to third parties harmed Plaintiffs by, among other things, consuming data for which Plaintiffs as part

---

[2] Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[3] BBC News, *Zoom Under Increased Scrutiny As Popularity Soars* (April 1, 2020), available at <https://www.bbc.com/news/business-52115434 (Last Visited July 28, 2020)> (Last Visited July 29, 2020).

[4] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account* (March 26, 2020), available at <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> (Last Visited July 28, 2020).

[5] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

of their carrier's plan,[6] causing wear and tear on the devices from which data is extracted, and diminishing the value of their personal information. Perhaps worst of all, Plaintiffs are harmed when their extracted data is used to target and profile them with unwanted and/or harmful content.

7. On March 31, 2020, an article in The Intercept revealed as false Zoom's claims that it implemented end-to-end encryption ("E2E")—widely understood as the most private form of internet communication—to protect the confidentiality of users' video conferences.[7] In fact, Zoom was using its own definition of the term, one that failed to recognize Zoom's ability to access unencrypted video and audio from meetings. Zoom's misrepresentations are a stark contrast to other videoconferencing services, such as Apple's FaceTime, which have undertaken the more challenging task of implementing true E2E encryption.

8. On April 2, 2020, the New York Times published an article disclosing "a data-mining feature" related to a LinkedIn application that could be used to snoop on participants during Zoom meetings without their knowledge.[8]

9. Finally, reports continue to the present day of security breaches during which unauthorized bad actors hijack Zoom videoconferences, displaying pornography, screaming racial epitaphs, or engaging in similarly despicable conduct. This practice has become so commonplace on the Zoom platform that it is referred to as "Zoombombing." Bad actors have disrupted private moments ranging from Alcoholics Anonymous meetings to

[6] Jeffrey Fowler, *In the middle of the night. Do you know who your iPhone is talking to?* (May 28, 2019), available at <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/> (Last Visited July 30, 2020).

[7] Micah Lee and Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading* (March 31, 2020), available at <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (Last Visited July 28, 2020).

[8] Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, New York Times (April 2, 2020), available at <https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html> (Last Visited July 28, 2020).

Holocaust memorial services (*e.g.*, in one instance with images of Adolf Hitler).[9] School classes and religious services all over the world have been affected. Recordings of these incidents and others end up on YouTube and TikTok with the horrified reactions of participants being the digital trophies of the Zoombombers. Concerns regarding Zoombombing led many organizations to ban employees' use of Zoom, including Google, SpaceX, NASA, the Australian Defence Force, the Taiwanese and Canadian governments, the New York Department of Education, and the Clark County School District in Nevada.[10]

10. The gravity of these data privacy violations cannot be overstated, including the data points leaked through the Facebook SDK. A growing and insidious practice in the "AdTech" industry to collect unique device data from consumers in order to build a profile, sometimes referred to as a "fingerprint," is used to allow third parties and data brokers to follow users' activities across their devices with essentially no limit. The practice of fingerprinting is unique and more damaging than the practice of tracking consumers' browsing activity with cookies.

11. Zoom had the affirmative duty to safeguard consumers' device information and, at the very minimum, to disclose the access, collection, and dissemination of consumers' data. Zoom failed to fulfill such duties.

12. Zoom users have an expectation of privacy in their videoconference communications, just as they do during telephone calls, irrespective of the substance of those communications. With social distancing and quarantine orders in place during the COVID-19 pandemic, videoconference platforms like Zoom have replaced conference rooms, churches and temples, AA meeting rooms, schools, and healthcare professionals' offices. The need for proper security with respect to private video conferences during which people

[9] Sebastien Meineck, *'Zoom Bombers' Are Still Blasting Private Meetings With Disturbing and Graphic Content* (June 10, 2020), available at <https://www.vice.com/en_us/article/m7je5y/zoom-bombers-private-calls-disturbing-content> (Last Visited July 28, 2020).

[10] *Id.*

discuss their religious views, struggle with addiction, where children are educated, and where healthcare professionals provide counsel, is paramount.

13. Zoom has issued mea culpas after the reports exposing its privacy inadequacies, admitting to the problems and vowing to change its ways.[11] Nonetheless, independent ratings organizations consider Zoom's commitment to security on par with some of the worst of today's tech giants.[12] Nonetheless, Zoom continues to exploit the ever-greater market share of the video conferencing that has become a daily necessity with state stay-at-home orders for attending class, practicing our faith, engaging with loved ones, and getting the advice of medical professionals. Ensuring privacy and safety during the use of Zoom's popular platform is a matter of public interest.

14. Each of these security lapses presents an independently actionable event. Data sharing relating to Facebook and LinkedIn incidents are breaches of common law, contract, and statutory duties to refrain from sharing and collecting users' valuable data without proper disclosures. Similarly, although they arise from the same freewheeling security practices, Zoom's misrepresentations regarding of E2E encryption and its security protocols to prevent Zoombombings, are independently actionable.

15. Zoom's popularity is such that it has become ubiquitous despite its security shortcomings. Despite knowledge of Zoom's shortcomings and a desire to maintain one's privacy, many people including Plaintiffs nonetheless are required to use Zoom for work, school, or other purposes, including. For instance, this Court has been using Zoom to conduct hearings remotely during the pandemic.[13]

---

[11] CEO Eric Yuan himself admitted that Zoom fell "short of our community's—and our own—privacy and security expectations." Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[12] As of May 2020, PrivacySpy gave Zoom a privacy score of 3.5 out of 10, similar to that of Facebook (3.2) and Amazon (3.5). *See* <https://privacyspy.org/product/zoom/> (Last Visited July 28, 2020).

[13] *See* Northern District of California, *Preparing to Participate in a Zoom Video Conference*, available at <https://www.cand.uscourts.gov/zoom/> ("Participants: If you do not already have a Zoom account, set one up at https://zoom.us.") (Last Visited July 30, 2020).

16. Accordingly Plaintiffs, on behalf of themselves and all others similarly situated, bring this action to ensure that Zoom vastly improves its security practices going forward and to recover for past privacy violations.

PARTIES

17. **Plaintiff Kristen Hartmann** is, and at all times relevant was, a citizen of the State of Maryland residing in Rockville, Maryland. Ms. Hartmann purchased a "Zoom Pro" account for her own personal use at a cost of $14.99 per month, and accessed Zoom's video conferencing services.

18. Ms. Hartmann was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing and behavior influencing purposes. Rather, Ms. Hartmann registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Hartmann did not give Zoom permission to access, take or use her personally identifiable information.

19. Ms. Hartmann purchased her account having seen advertising that Zoom Meetings were equipped with end-to-end encryption technology, which was a feature that she valued and for which she was willing to pay a premium. After comparing Zoom against GoToMeeting and Webex, Ms. Hartmann selected Zoom over other options largely due to Zoom's representations of its end-to-end encryption. Further, periodically during Zoom meetings calls, Ms. Hartmann would "check" to ensure the calls were end-to-end encrypted by hovering her cursor over the green lock icon in the application. The icon would then show text indicating active end-to-end encryption. Had Ms. Hartmann known that Zoom

meetings were not actually end-to-end encrypted, she would not have paid for a Zoom Pro subscription, or she would have paid less for it.

20. **Plaintiff Isabelle Gmerek** is, and at all times relevant was, a citizen of the State of California residing in Carlsbad, California. Ms. Gmerek has registered an account with Zoom, and accessed Zoom's video conferencing services.

21. Ms. Gmerek was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Gmerek registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Gmerek did not give Zoom permission to access, take or use her personally identifiable information.

22. In late February or early March of 2020, Ms. Gmerek began using Zoom for meetings with her psychologist in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), and that it had not misrepresented the security features available to users.

23. Ms. Gmerek uses Zoom at least twice a week as an attendee, but she has no way of determining whether Zoom's representations that her personal information will be secure are, in fact, correct.

24. **Plaintiff Lisa T. Johnston** is, and at all times relevant was, a citizen of the State of California residing in Santa Monica, California. Ms. Johnston has registered an account with Zoom, and accessed Zoom's videoconferencing services.

25. Ms. Johnston was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Johnston registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Johnston did not give Zoom permission to access, take or use her personally identifiable information.

26. **Plaintiff M.F.** is, and at all times relevant was, a citizen of the State of California residing in Culver City, California. M.F. accessed Zoom's video conferencing services without first creating a Zoom account. M.F. is, and at all relevant times was, under the age of 13.

27. M.F. was not aware, and did not understand, that Zoom would collect and share his personal information with third parties, including Facebook. Nor was he aware that Zoom would allow third parties, like Facebook, to access his personal information and combine it with content and information from other sources to create a unique identifier or profile of his for advertising and behavior influencing purposes. Rather, M.F. used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, M.F. did not give Zoom permission to access, take or use his personally identifiable information.

28. **Plaintiff Therese Jimenez** is, and at all times relevant was, a citizen of the State of California residing in Culver City, California. Ms. Jimenez accessed Zoom's video

conferencing services without first creating a Zoom account. Plaintiff Jimenez is the mother and natural guardian of Plaintiff M.F.

29. Ms. Jimenez later registered with Zoom as a user. When she did so Ms. Jimenez was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Jimenez registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Jimenez did not give Zoom permission to access, take or use her personally identifiable information.

30. **Plaintiff Saint Paulus Lutheran Church** is, and at all times relevant was, a citizen of the State of California.

31. Saint Paulus Lutheran Church is an Evangelical Lutheran church located at 1541 Polk Street, San Francisco, California. Founded in 1867, Saint Paulus has been serving countless congregants, including the homeless, the marginalized, and the underserved, in San Francisco for over 150 years. The Reverend Daniel Solberg has served as the eighth Pastor of Saint Paulus Lutheran Church since November of 1999. Saint Paulus is a citizen of California. In Saint Paulus's long history, it survived the Great Earthquake and Fire of 1906, the social and cultural turmoil of the 1960s–70s, and a 1995 fire that destroyed its 103 year-old cathedral building.

32. **Plaintiff Heddi N. Cundle** is, and at all times relevant was, a citizen of the State of California residing in San Francisco, California. She is the administrator at Saint Paulus. She organizes Saint Paulus's weekly bible-study classes. Ms. Cundle registered an account with Zoom on behalf of Saint Paulus, and accessed Zoom's videoconferencing on

behalf of Saint Paulus. Ms. Cundle also registered a separate account with Zoom for personal use, and accessed Zoom's videoconferencing for personal purposes.

33. Ms. Cundle was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Cundle registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Cundle did not give Zoom permission to access, take or use her personally identifiable information.

34. Further, Ms. Cundle on behalf of Saint Paulus was not aware, and did not understand, that Zoom would collect and share Saint Paulus's private information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access Saint Paulus's private information and combine it with content and information from other sources to create a unique identifier or profile of Saint Paulus for advertising purposes. In fact, Ms. Cundle on behalf of Saint Paulus registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Cundle on behalf of Saint Paulus did not give Zoom permission to access, take or use its personally identifiable information.

35. To conduct Saint Paulus's weekly Bible-study class in compliance with the State's stay-at-home order, Ms. Cundle registered an account with Zoom on behalf of Saint Paulus. Saint Paulus paid a monthly fee of $14.99 per month for its Zoom account. Through

Ms. Cundle and congregants, Saint Paulus has continued to use and access Zoom videoconferencing services.

36. For the May 6, 2020 Saint Paulus Bible-study class, Ms. Cundle followed Zoom's instructions to set up a password-protected meeting. Despite her efforts, an intruder hacked into the Bible-study meeting and hijacked the meeting, displaying child pornography images and video to the participants. During the Zoombombing incident, Ms. Cundle and the other participants were unable to minimize or close the video screen. Despite Ms. Cundle's efforts to use the tools Zoom made available to her, she could not stop the graphic display or eject the intruder and, thus, closed the meeting and instructed the participants to rejoin. As soon as participants rejoined, the intruder again hijacked the Bible study with further displays of child pornography. Despite Ms. Cundle's efforts to use the tools Zoom made available to her, she could not stop the graphic display or eject the intruder and, thus, after attempting, unsuccessfully, to block the intruder or close the meeting, she finally closed the meeting. The depravity of the video footages was beyond description here. Ms. Cundle and the other participants were traumatized and deeply disturbed.

37. Immediately following the May 6, 2020 Zoombombing incident, Ms. Cundle reported the incident to Zoom. In response, Zoom admitted that the intruder was "a known serial offender who disrupts open meetings by showing the same video" and, shockingly, had "been reported multiple times to the authorities." Despite this, it was not until Ms. Cundle reported the May 6, 2020 Zoombombing incident that Zoom finally blocked the intruder "from joining future meetings using the same Zoom software."

38. **Plaintiff Oak Life Church** is, and at all relevant times was, a citizen of the State of California. Oak Life Church is located at 337 17th Street, Oakland, California. Founded in 2014, Oak Life Church is a decentralized, non-denominational Christian church serving the marginalized and the underserved in the community. Beginning in March 2020, Oak Life Church registered an account with Zoom, which it subsequently converted to a "Zoom Pro" account at a cost of $14.99 per month. Thereafter, Oak Life Church accessed

Zoom's videoconferencing services for team meetings, Bible studies, prayer meetings, and church services.

39. Oak Life Church was not aware, and did not understand, that Zoom would collect and share its private information with third parties, including Facebook. Nor was Oak Life Church aware that Zoom would allow third parties, like Facebook, to access its private information and combine it with content and information from other sources to create a unique identifier or profile of Oak Life Church for advertising purposes. In fact, Oak Life Church registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Oak Life Church did not give Zoom permission to access, take or use its personally identifiable information.

40. On April 19, 2020, Oak Life Church and its members were subjected to a Zoombombing incident during a regularly-scheduled Sunday church service. Following protocols provided by Zoom, the meeting on April 19, 2020 was set up with a waiting room, mute on entry, and no ability for users to share their screens. Thirty minutes into the service, while the host was using Zoom's screen-sharing feature, the host's dedicated screen started to experience issues, whereby a "black box" appeared on the host's screen, covering the image being projected to other meeting participants. When efforts to fix the issue were unsuccessful, the host stopped the screen sharing. Shortly thereafter, the Zoombombing incident took place, whereby child pornography images and video were displayed to the participants. After attempting, unsuccessfully, to block the intruder, the host shut down the meeting as quickly as possible. But the damage was done. The participants from that meeting, many of whom were trauma survivors to begin with, were left traumatized and devastated. Oak Life Church was required to hire trauma counsellors and establish support groups to assist its congregation in dealing with the resulting trauma.

41. Immediately following the April 19, 2020 Zoombombing incident, Oak Life Church reported the incident to Zoom. In response, Zoom admitted that the intruder was a "known offender" and that the intruder had used the same IP address to attack Zoom's network before. Despite this, it was not until Oak Life Church reported the April 19, 2020 Zoombombing incident that Zoom finally "blocked the offender from joining future meetings using the same Zoom software."

42. **Plaintiff Stacey Simins** is, and at all times relevant was, a citizen of the State of Texas residing in Austin, Texas. Ms. Simins purchased a "Zoom Pro" account at a cost of $14.99 per month, and accessed Zoom's videoconferencing services.

43. Ms. Simins was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Simins registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Simins did not give Zoom permission to access, take or use her personally identifiable information.

44. Ms. Simins is the operator of a burlesque dance studio and uses her Zoom Pro account for teaching classes. On multiple occasions, uninvited men showed up in dance classes taught by her studio. These men were present in the dance classes for several minutes before Ms. Simins shut down the meeting. As a result, Ms. Simins lost a significant portion of her clientele; 10-15 full time members and any new clients who were present for the incidents will no longer participate in online classes.

45. **Plaintiff Caitlin Brice** is, and at all times relevant was, a citizen of the State of Illinois residing in Chicago, Illinois. Ms. Brice registered an account with Zoom for personal

use, and accessed Zoom's videoconferencing series for personal use. Ms. Brice also access Zoom's videoconferencing services through a paid account maintained by her employer for work purposes.

46. Ms. Brice was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Brice registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Brice did not give Zoom permission to access, take or use her personally identifiable information.

47. In August or September 2018, Ms. Brice began using Zoom for speech therapy meetings with her students in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with HIPAA, and that it had not misrepresented the security features available to users.

48. In April or May 2020, Ms. Brice attended a Zoom event during which the participants were subjected to intentional pornographic material when unknown men dropped into the meeting with the intention of disrupting it.

49. **Plaintiff Cynthia Gormezano** is, and at all times relevant was, a citizen of the State of New York residing in New York, New York. Ms. Gormezano's physical therapy clinic purchased a "Zoom Pro" account at a cost of $14.99 per month, and Ms. Gormezano accessed Zoom's videoconferencing services.

50. Ms. Gormezano was not aware, and did not understand, that Zoom would collect and share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a

unique identifier or profile of her for advertising and behavior influencing purposes. Rather, Ms. Gormezano registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures. Likewise, Ms. Gormezano did not give Zoom permission to access, take or use her personally identifiable information.

51. In March of 2020, Ms. Gormezano began using Zoom for meetings with her patients in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), and that it had not misrepresented the security features available to users.

52. **Defendant Zoom Video Communications, Inc.** is a Delaware corporation with its principal place of business and headquarters in San Jose, California.

JURISDICTION AND VENUE

53. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

54. This Court has personal jurisdiction over Defendant because it is headquartered in California, and regularly conducts business in California.

55. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

STATEMENT OF FACTS

ZOOM AND ITS SERVICES

56. Zoom provides a cloud-based communications platform for video and audio conferencing to both business and individual consumers throughout California and the United States. Zoom's products and services can be used across mobile devices, desktops, telephones, and room systems.

57. Zoom purports to provide "[s]implified video conferencing and messaging across any device."[14]

58. Zoom offers different tiers of services for its registered users: Basic, Pro, Business, and Enterprise. Subscription fees range from free for the Basic version, to $19.99 per month per user for the Enterprise version.[15] While users receive additional features under more expensive subscriptions, Zoom's representations regarding the security of its video conferences and its published privacy policy with its representations regarding data sharing are common to all subscription levels.

59. Since its founding, Zoom boasted that its platform has been used to conduct tens of billions of meeting minutes.[16]

60. Zoom has developed mobile apps to access its most popular service, Zoom meetings, for both the iPhone and Android. Zoom provides software to access Zoom meetings on a desktop computer for both Windows and Mac operating systems. Further add-ons, add-ins, plugins, and extensions are available for Microsoft Office 360, Outlook, Gmail, Firefox, Chrome, and Safari.

61. Parties who host a Zoom meeting invite participants in one of two ways. First, a host may utilize a Zoom feature whereby Zoom will link to the host's email account directly

[14] <https://zoom.us/meetings> (Last Visited July 28, 2020).

[15] <https://zoom.us/pricing> (Last Visited July 28, 2020).

[16] Zoom Video Communications, Inc. Form S-1 (March 22, 2019), available at <https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm> (Last Visited July 28, 2020).

and provide a form email containing the URL for participants of the Zoom meeting to use, or by otherwise providing that URL for participants to enter into their web browser.

62. Alternatively, Zoom provides a telephone number and access code for participants who wish to call with a telephone as a voice-only participant.

63. Users who have a Zoom app on their computer or cellphone are directed to that app after clicking on the URL. User who do not have the Zoom app are directed to a Zoom webpage where the meeting is hosted. Voice-only telephone users participate in the meeting as one would with a normal telephone conference call, *i.e.* without employing any app or webpage.

64. In March 2019, Zoom boasted that its platform "has been used to conduct tens of billions of meeting minutes" since its founding in 2011.[17] In early 2020, usage of video conferencing increased even more dramatically in response to the coronavirus pandemic, and Zoom's usage surged higher. As of the end of December 2019, Zoom had a maximum number of 10 million daily meeting participants, both free and paid. In March 2020, Zoom reached more than 200 million daily meeting participants, both free and paid.[18]

DATA SHARING, DEVICE FINGERPRINTING, DATA MINING, AND ZOOM'S PRIVACY POLICY

Facebook Data Sharing

65. On March 26, 2020, Joseph Cox posted an article on Vice Media Group's website Motherboard revealing that the Zoom iPhone app sends data to Facebook even if the Zoom user does not have a Facebook account.[19] The article states "The Zoom app notifies Facebook when the user opens the app, details on the user's device such as the model, the time zone and city they are connecting from, which phone carrier they are using,

---

[17] *Id.*

[18] Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[19] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account* (March 26, 2020), available at <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> (Last Visited July 28, 2020).

and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements." The article continues that Zoom confirmed the data collection several days after it was asked for comment and a day after the publication of the article.

66. On March 27, 2020, Zoom's Founder and Chief Executive Officer, Eric Yuan, published a statement asserting that Zoom was unaware until two days prior that its Zoom iPhone app was providing any of its users' personal data to Facebook. Nevertheless, Mr. Yuan represented that Zoom "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to us."[20]

67. Mr. Yuan stated that the data sharing was the result of Zoom's use of the Facebook software developer kit ("SDK").[21] An SDK is a collection of software development tools in one installable package. The Facebook SDK allows mobile app developers to integrate Facebook tools (like "Login with Facebook" and Facebook Analytics Tools) within the mobile app. They ease creation of applications, because the code has already been written and debugged by the provider of the SDK (in this case Facebook). Due to the nature of how Facebook's SDKs are implemented by parties such as Zoom, any data collected via the SDK is, by default, automatically passed to Facebook, allowing Facebook to keep a log of app usage.

68. Use of the Facebook SDK is voluntary for the convenience of app developers. It is used not only to offer the "Log in with Facebook" feature, but also to track user actions within the application, traffic to and within the application. SDKs are valuable to developers because they allow companies that use the SDK to build profiles on their users. In exchange for this built and packaged software, Facebook receives that same data Zoom collected using Facebook's SDK, and in turn sells the data to marketers and data brokers.

[20] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

[21] *Id.*

69. Mr. Yuan confirmed that users' personal data released to Facebook included: Application Bundle Identifier; Application Instance ID; Application Version; Device Carrier; iOS Advertiser ID; iOS Device CPU Cores; iOS Device Disk Space Available; iOS Device Disk Space Remaining; iOS Device Display Dimensions; iOS Device Model; iOS Language; iOS Timezone; iOS Version; and IP Address.[22] An updated version of the Zoom app was released which would prevent the release of information to Facebook. Users were encouraged, but not required, to update to this newer version of the Zoom app.

70. The bulleted list on Zoom's March 27, 2020 blog was apparently not even a complete disclosure of all information that was passed to Facebook. Mr. Yuan stated that the list was only "examples" of data shared with Facebook without explaining why the entire list of shared data was not provided. Facebook's online handbook for developers states that the Facebook SDK is not limited to information reported by Zoom, but also includes "explicit events, implicit events, and automatically logged events, Facebook app ID," and potentially even more information.[23] The range of information this description could include is staggering.

71. From the very first install and launch of an app (such as Zoom) that utilizes Facebook's SDK, data is sent to Facebook. This happens regardless of whether the user has created a Zoom or Facebook account, and, even worse, before the user would have even encountered Zoom's terms and conditions or any privacy disclosures. Furthermore, the data sharing occurs even if someone has "opted out" of social media and advertising for that particular app.

72. Even for individuals without a Facebook account, a shadow profile is built based on a compilation of app usage on the specific individual's device. Every interaction someone has through apps installed on their device (that utilize Facebook's SDKs) is logged and sent to Facebook. The data is then correlated, aggregated, and shared back to Facebook

[22] *Id.*

[23] <https://www.facebook.com/business/m/one-sheeters/gdpr-developer-faqs> (Last Visited July 29, 2020).

partners. The more complete the profile, the more monetary value it holds on the personal data market.

73. Facebook starts receiving data on its servers the second the installation process begins on the device. Following the adoption of the European Union's Data Protection Regulation ("GDPR") in 2018, Facebook SDK started to allow developers to disable automatically logged events like app installation and login. However, developers must manually and deliberately go into the code and change the default settings. Based on public statements made by Zoom, Plaintiffs are informed and believe that Zoom did not change this default setting. Thus, Facebook was receiving this information before users ever had access to any terms and conditions or privacy disclosures.

74. When initially starting an application, the Facebook SDK gets invoked several times, but one particular invocation sends an "Application Install" as an "event" to the Facebook Graph API (Application Programming Interface) detailing:

- the user's IP Address, allowing Facebook to Geo-Reference your location and correlate your device with other devices using the same IP Address;
- Advertiser_id, a unique identifier shared across all applications installed on the user's device, which allows advertisers to link data about the user and to correlate most of that data;
- device model, screen resolution, and system language;
- carrier name and timezone, allowing Facebook not only to know your location through IP Address, but also if you are traveling or roaming; and
- the origin of the application (or the App Store), allowing Facebook to learn whether the user installed this app from the Manufacturer's store or elsewhere.

75. All these data points create a fingerprint of the user's identity.

Device Fingerprinting

76. Zoom attempted to downplay the personal-identifying nature of the information released to Facebook. Mr. Yuan stated that the data sent to Facebook's servers

was not related to Zoom conference attendees but, "rather, included information about devices . . . ." This is misleading because not only is the shared information used to "fingerprint" the user's identity as explained below but, when combined with information regarding other apps used on the same device, this information is used to build extremely precise and detailed profiles on individuals, ultimately identifying characteristics such as race, age, sexual orientation, relationship status, socioeconomic status, parental status, and much more.

77. Fingerprinting is a process by which websites and applications can discern that a device belongs to a particular user based on system configurations. Fingerprinting makes it extremely difficult for individuals to give informed consent about the way their data is collected and used. Promises made by companies not to share personally identifiable information are meaningless when it's so easy to re-identify someone.

78. SDKs like those used by Zoom for iOS are like the mobile equivalent of cookies, but with more power because the apps are on the device itself. Cookies are a piece of code that is saved on a consumer's own browser that sends information to various third parties that are able to use the cookies to obtain information about the consumer's browsing activity. Consumers can remove the cookies cached in their browser through various options built into their browsers. Many browsers also give consumers the ability to block all cookies—so first party publishers and third-party data brokers are not able to place cookies in the consumers' browsers or retrieve data from them.

79. Device fingerprinting using mobile apps (in contrast to web pages) is nefarious because the practice gives consumers no choice about whether the websites they visit, or third parties, can observe their internet activity. A device fingerprint is created with the exact types of data that Zoom provided through its iOS app and its use of the Facebook SDK. Information such as iOS Advertiser ID and iOS Device Display Dimensions are so unique to each user that the information, in combination with the user's IP address or other data, creates a profile or "fingerprint" unique enough that Zoom and third parties such as Facebook can use the unique identifier to observe a consumer's internet browsing activity

regardless of whether that person clears their cookies, blocks cookies, or uses private browsing.

80. Consumer device data, such as that leaked by Zoom, is especially valuable because consumers increasingly block cookies and take precautions against cookie tracking. The device data enables fingerprinting, an even more powerful tracking tool than cookies.

81. Even tech giants admit that device fingerprinting is wrong. Indeed, the director of Chrome Engineering at Google stated regarding fingerprinting in an August 2019 blog post:

> With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites. Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected. We think this subverts user choice and is wrong.[24]

Data Sharing With Google

82. Facebook isn't the only third party receiving detailed user data from Zoom. Even though Zoom reports it removed the Facebook SDK, the application is still sharing data with Google according to a July 13, 2020 Exodus report. Zoom shares information with Google via the Google Firebase Analytics tracker. A tracker is a piece of software that gathers information on the person using the application or on the smartphone being used. A tracker typically is distributed as an SDK, just as discussed in the Facebook context.[25]

83. Zoom allows Google the following permissions and access (among many things):

- GPS (precise) and network-based (approximate) location
- "Do Not Disturb" setting

[24] Justin Schuh, *Building a More Private Web* (Aug. 22, 2019), available at <https://www.blog.google/products/chrome/building-a-more-private-web/> (Last Visited July 29, 2020).

[25] *See* <https://reports.exodus-privacy.eu.org/en/reports/us.zoom.videomeetings/latest/> (Last Visited July 30, 2020).

- Available wi-fi connections
- Bluetooth settings
- Read your Calendar and Details
- Read your Contacts
- Read contents of SD card
- Read phone status and identity

84. Depending on the smartphone and operating system, it is sometimes possible for users to restrain some of these permissions, but the vast majority of users have no idea the specific permissions allowed by default.

Data Is the New Oil

85. Data harvesting is the fastest growing industry in the entire country. As software, data mining, and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

86. Consumer data is so valuable that some have proclaimed that data is the new oil.[26] Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, internet companies earned $202 per American user. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate.[27]

87. Both Facebook and Google are established personal data brokers. Data is monetized through targeted advertising. Facebook's ability to sell targeted messaging to its

[26] *The World's Most Valuable Resource Is No Longer Oil, But Data*, The Economist (May 6, 2017), available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (Last Visited July 29, 2020).

[27] R Shapiro, *What Your Data Is Really Worth to Facebook*, Washington Monthly (July/Aug. 2019), available at <https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/> (Last Visited July 29, 2020); *see also* R Shapiro & A Siddhartha, *Who owns American's Personal Information and What is it Worth?*, available at <https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf> (Last Visited July 29, 2020).

user population now drives its revenues and share price. But beyond profiting from direct advertising, both Facebook and Google also enter into data sharing/selling partnerships with various companies and apps where the entire basis of the deal is around the value of data extracted from apps like Zoom. Facebook in particular engineered its SDKs and APIs to facilitate the collection of data for app developers and for its business partners like Apple, Samsung, Amazon and other third parties.

88. Facebook's partnerships with third parties, including device makers and its app developers, have formed a large part of its data-brokerage strategy. These partnerships allow Facebook to pool and aggregate information about billions of people for the purpose of targeting them with content. By engaging in partnerships with third party app developers, mobile devices makers, software makers, security firms, and even the chip designer Qualcomm, Facebook leveraged its position as a curator of user content and information.

89. For example, data sharing partners of Facebook such as cellular network carriers and device designers use this data to assess their standing against competitors, including customers lost to and won from those competitors.

90. In 2018, Facebook introduced "Actionable Insights," a corporate data sharing program including operators, carriers, internet service providers, and device makers to "enable better business decisions" through "analytics tools." It's exactly this sort of quasi-transactional data access that has become a hallmark of Facebook's business, allowing the company to plausibly deny that it ever sells data while still leveraging it for revenue.

91. Facebook itself also has an interest in technical information collected about devices that goes beyond social media. Since 2013, Facebook has been working towards establishing itself as a network service provider through efforts such as Facebook Connectivity and Fiber. Facebook now offers high capacity fiber-optic routes to sell unused capacity between its data centers to third parties.

92. It's no secret that Facebook also seeks to become a frontrunner in the videoconferencing sector. On July 23, 2020, Facebook announced that it is "launching its

own Zoom competitor."[28] Technical device and performance information collected by the SDK is quite valuable to Facebook's efforts in this regard. "The Video Engineering team at Facebook is responsible for the end-to-end video experience, including upload, encoding, playback, and distribution across mobile and web. From backend infrastructure like networking and storage to the software that supports product development, our work focuses on developing systems to deliver a world-class video experience at scale on all platforms."[29]

LinkedIn Data Mining

93. In November 2018, Zoom integrated the LinkedIn Sales Navigator Application Platform ("SNAP"). Through applications such as SNAP available on Zoom's App Marketplace, Zoom increases the value to customers by allowing them to leverage LinkedIn Sales Navigator to see who was attending meetings. According to Zoom: "The service uses the participant's email and name to match to their LinkedIn Sales Navigator profile."[30] Upon release, head of platforms at Zoom explained: "This integration adds tremendous value to Zoom.[31]

94. The app was available to Zoom users who subscribed to a LinkedIn service for sales prospecting, called LinkedIn Sales Navigator. Once a Zoom user enabled the app, that user could quickly and covertly view LinkedIn profile data—like locations, employer names and job titles—for people in the Zoom meeting by clicking on a LinkedIn icon next to their name.

95. The system did not simply automate a manual process of looking up the name

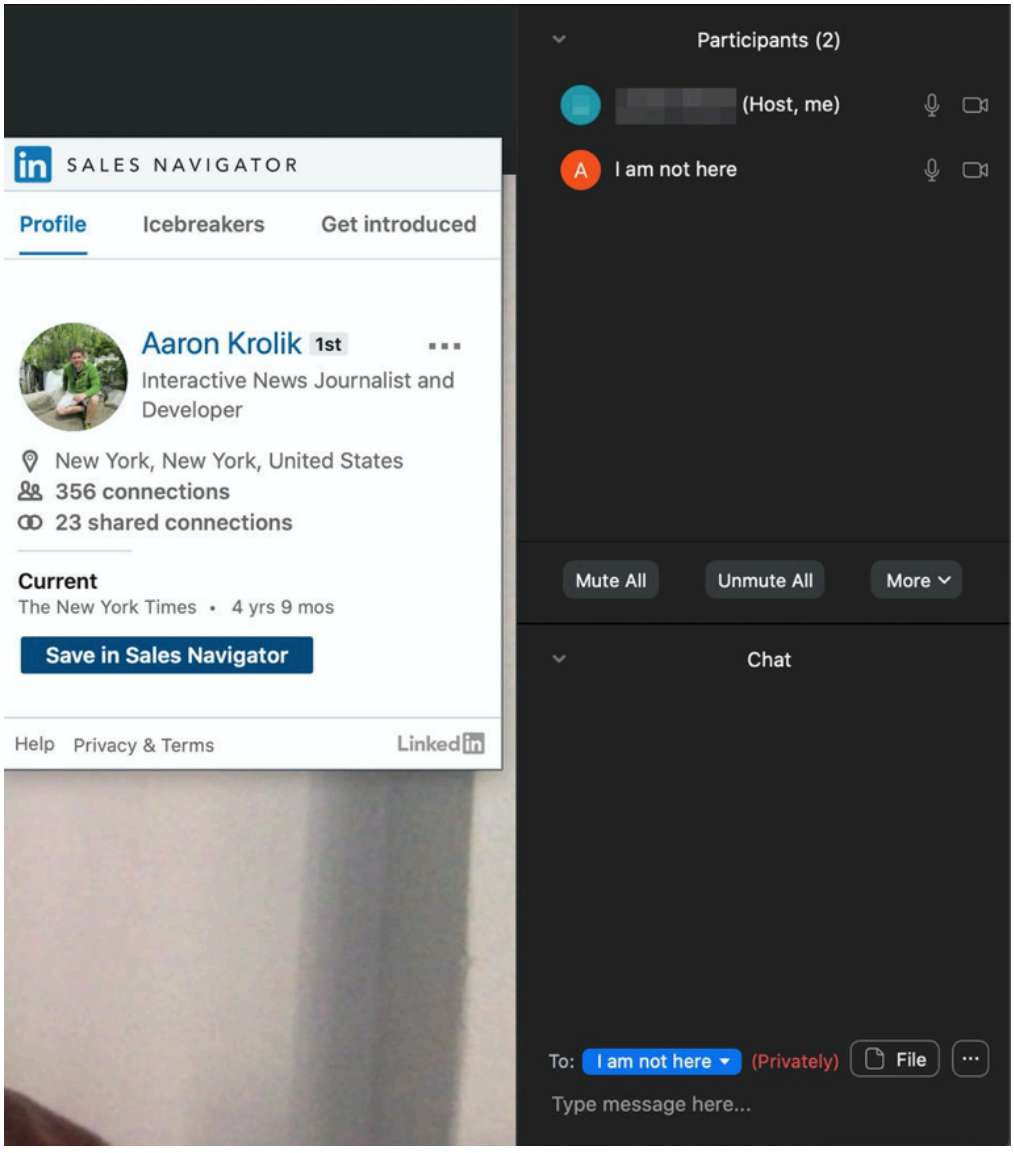
[28] Alison Durkee, *Facebook Is Launching Its Own Zoom Competitor*, Forbes (July 23, 2020), available at <https://www.forbes.com/sites/alisondurkee/2020/07/23/facebook-is-launching-its-own-zoom-competitor/#4be9bdfe2495> (Last Visited July 29, 2020).

[29] https://engineering.fb.com/category/video-engineering/ (Last Visited July 29, 2020).

[30] Priscilla Barolo, LinkedIn Sales Navigator Integration is the Latest Addition to Zoom App Marketplace (Nov. 14, 2018), available at <https://blog.zoom.us/linkedin-sales-navigator-integration-is-the-latest-addition-zoom-app-marketplace/> (Last Visited July 29, 2020).

[31] *Id.*

of another participant on LinkedIn during a Zoom meeting. Tests conducted by the New York Times found that even when reporter Aaron Krolik signed into a Zoom meeting under pseudonyms "Anonymous" and "I am not here" the datamining tool was able to instantly match him to his LinkedIn profile. In doing so, Zoom disclosed Mr. Krolik's real name to another user, overriding his efforts to keep his name private:[32]



[32] Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles,* New York Times (April 2, 2020), available at <https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html> (Last Visited July 28, 2020).

96. Reporters also found that Zoom automatically sent participants' personal information to its data-mining tool even when no one in a meeting had activated that tool. For instance, as high school students in Colorado signed into a mandatory video meeting for a class, Zoom prepared a list of full names and email addresses of at least six students and their teacher. Zoom likely uses this information to integrate the various apps available on its App Marketplace, including the LinkedIn Sales Navigator app.

97. Zoom explicitly misleads customers and consumers into believing their information is secure on Zoom's platform. As described by one Zoom developer in a July 2019 Medium post, "more importantly, users needed to trust these apps. Because our customers use these apps, we developed a rigorous process around security-focused testing and validation. For example, we prevent apps from pulling customer or end-user data without explicit consent and approval."[33] This was not the case.

98. As with the data gathered through the Facebook SDK, the names and email address of meeting participants is valuable in and of itself. However, when paired with other profiles, *e.g.*, those maintained by LinkedIn, the data has extraordinary value for all sorts of commercial and illegitimate purposes.

Zoom's Privacy Policy

99. Zoom maintains what it describes as "marketing" websites, *e.g.*, zoom.us and zoom.com, where its Privacy Policy is available. Zoom's privacy policies have had three iterations that were complete overhauls of its previous versions: pre-March 29, 2020 policy, post-March 29, 2020 policy, and post July 2020 policy.

100. Prior to March 29, 2020, Zoom's Privacy Policy stated:

> **Collection of your Personal Data**
>
> Whether you have Zoom account or not, we may collect Personal Data from or about you when you use or otherwise interact with our Products. We may gather the following categories of Personal Data about you:

[33] Tim Sagle, *Zoom App Marketplace — What We Learned and Where We're Going* (July 23 ,2019), available at <https://medium.com/zoom-developer-blog/zoom-app-marketplace-what-we-learned-and-where-were-going-9e15882794ca> (Last Visited July 28, 2020).

- Information commonly used to identify you, such as your name, user name, physical address, email address, phone numbers, and other similar identifiers
- Information about your job, such as your title and employer
- Credit/debit card or other payment information
- Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)
- General information about your product and service preferences
- Information about your device, network, and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version
- Information about your usage of or other interaction with our Products ("Usage Information")
- Other information you upload, provide, or create while using the service ("Customer Content"), as further detailed in the "Customer Content" section below[34]

101. Zoom's pre-March 29, 2020 Privacy Policy continues:[35]

> Mostly, we gather Personal Data directly from you, directly from your devices, or directly from someone who communicates with you using Zoom services, such as a meeting host, participant, or caller. Some of our collection happens on an automated basis – that is, it's automatically collected when you interact with our Products.

102. Finally, Zoom's pre-March 29, 2020 Privacy Policy states: "We may also obtain information about you from a user who uses Zoom."[36]

103. On March 29, 2020, Zoom's Chief Legal Officer, Aparna Bawa, released a statement that: "We are not changing any of our practices. We are updating our privacy policy to be more clear, explicit, and transparent."[37] This statement linked to a broadly revised Zoom Privacy Policy that included both more and less clarity but it still asserted that "[t]he categories of data we obtain when you use Zoom include data you provide to us as

---

[34] Zoom Privacy Policy (February 23, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200311205042/https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (February 23, 2020)").

[35] *Id.*

[36] *Id.*

[37] Aparna Bawa, *Zoom's Privacy Policy* (March 29, 2020), available at <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/> (Last Visited July 28, 2020).

well as data that our system collects from you" and that "'You' or 'user' or 'participant' is anyone who uses Zoom" regardless of whether they have an account.[38]

104. In July 2020, Zoom again completely revised its privacy policy to include a chart of data usage which would be indecipherable to the average Zoom user. Language used to describe the type of data, and Zoom's intended use of that data, only raises more questions. For instance Zoom states that, "Automatically through use of the Service," it collects "Operation Data" which includes:[39]

- Configuration Data: information about the deployment of Zoom Services and related environment information.
- Meeting metadata: metrics about when and how meetings were conducted.
- Feature Usage Data: information about if and how Service features were used.
- Performance Data: metrics related to how the Services perform.
- Service Logs: information on system events and states.

105. Zoom's July 2020 privacy policy chart continues that any of these broad categories of "Operation Data" can be used to, among other things, "Create anonymized and/or aggregated data to improve our products and *for other lawful business purposes*"[40] (emphasis added). There is no further explanation of what Zoom considers a "lawful business purpose" or how a user is to understand this exception that swallows the preceding limitations to data usage Zoom outlines.

106. Zoom's March 29, 2020 privacy policy revealed that personal data collected from users included, but was not limited to: information that identifies you (name, username and email address, or phone number); technical information about your devices, network, and internet connection (IP address, MAC address, other device ID (UDID), device type,

[38] Zoom Privacy Policy (March 29, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200331032821/https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (March 29, 2020)").

[39] Zoom Privacy Policy (July 2020), available at <https://zoom.us/privacy> (Last Visited July 28, 2020) ("Zoom Privacy Policy (July 2020)").

[40] *Id.*

operating system type and version, client version, type of camera, microphone or speakers, connection type); approximate location; and other forms of metadata.[41] The July 2020 privacy policy chart both removed much of these details and revealed that Zoom has access to an additional range of information that includes billing information, employer information, and marketing data.[42]

107. The July 2020 included a disclosure at the bottom asserting that in revising Zoom's privacy policy on March 29, 2020, and again in July 2020: "We did not change or add any data practices, only how we described them."[43]

108. Accordingly, Zoom stands by its prior representation in its March 29, 2020 privacy policy that: "We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment. We do not allow third parties to use any personal data obtained from us for their own purposes, unless you consent (e.g., when you download an app from the Marketplace)."[44]

109. Zoom's revised July 2020 privacy policy also states that: "Zoom is committed to protecting your personal data. We use reasonable and appropriate technical and organizational measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data."[45]

110. Plaintiffs are informed and believe that Zoom has not complied with its own Privacy Policy by, among other things, sharing personal data from people engaging with its products to third parties, including but not limited to Facebook and LinkedIn.

111. Zoom users who have not been notified by Zoom's March 27, 2020 statement that its iPhone app was providing users' personal data to Facebook, and have thus not

[41] Zoom Privacy Policy (March 29, 2020).

[42] Zoom Privacy Policy (July 2020).

[43] *Id.*

[44] Zoom Privacy Policy (March 29, 2020).

[45] Zoom Privacy Policy (July 2020).

updated to the newer version of the Zoom iPhone app, continue to have their information released to Facebook.

112. Furthermore, many Zoom users would never have known of Zoom's policies on collection and dissemination of users' personal data. Zoom's disclosure of its Privacy Policy—and its collection and dissemination to third parties of users' personal data—is only available through a small link on Zoom's marketing page. Zoom users who opened an account prior to July 2020 would not have encountered the updated Privacy Policy by simply opening the Zoom app on their desktop or mobile device. Zoom users who have not opened a Zoom account have never been provided the Zoom Privacy Policy, nor is it likely they have ever even seen the Zoom marketing page since these users are automatically placed in a Zoom meeting after clicking the provided URL.

113. While Zoom continues to represent that it "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to" it, Zoom's actions demonstrate otherwise.[46] Zoom has attempted to sidestep liability by offering an update to its Zoom iPhone app through a blog post on its website without affirmatively contacting current users, or requiring users to update their Zoom iPhone app, and by revising its Privacy Policy to further obscure that users without accounts are having their data collected by Zoom and shared with third parties.

114. Had Zoom informed its accountholders that it would not engage in a thorough review of the third parties with whom its Zoom iPhone app shared personal data, *e.g.*, Facebook, LinkedIn, and other Zoom users, it is likely that customers—like Plaintiffs and Class members—would not have been willing to purchase its services at the price charged, or even to have used those services at all, regardless of price.

115. Zoom's failure to implement adequate security protocols or app review procedures jeopardized millions of consumers' privacy, fell well short of its promises, and

[46] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (March 27, 2020), available at <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> (Last Visited July 28, 2020).

diminished the value of the products and services provided. In other words, because Defendant failed to disclose its gross security inadequacies, and affirmatively shared users' information with third parties without their informed consent, it delivered fundamentally less useful and less valuable products and services than those for which consumers like Plaintiffs paid and/or expected when they chose to use them.[47]

116. While Zoom's wrongful conduct constitutes invasion of privacy in and of itself, entitling consumers to damages, Plaintiffs and Class members also now are placed at an increased risk of further imminent harm as a direct result of Zoom's wrongful acts and omissions. Indeed, a recent reports revealed that account information belonging to over half a million Zoom users was published, exchanged and, in some cases, sold online without their knowledge or consent.[48] No doubt this is a result of the aforementioned wrongful conduct by Zoom.

117. Finally, the unauthorized access to Plaintiffs' and Class members' private and personal data also has diminished the value of that information resulting in the above described harm to its users.

Unauthorized Interception and Use of Video Sessions, Chats, and Transcripts

118. Zoom's pre-March 29, 2020 privacy policy provides that, regardless of whether the consumer has a "Zoom account or not, we may collect Personal Data from or about you when you use or otherwise interact with our Products," including "information you upload, provide, or create while using the service ('Customer Content'), as further

[47] Zoom has admitted to further security issues related to its products including: "Zoombombing"—incidents of harassment by unauthorized participants in a Zoom meeting; failure of Zoom to implement promised end-to-end encryption; privacy issues related to attendee tracking features; data disclosures to LinkedIn; etc. *See* Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[48] Lawrence Abrams, *Over 500,000 Zoom Accounts Sold On Hacker Forums, the Dark Web* (April 13, 2020), available at <https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/> (Last Visited July 28, 2020).

detailed in the 'Customer Content' section below."[49] In the later section, the policy provides "Customer Content is information provided by the customer to Zoom through the usage of the service. Customer Content includes the content contained in **cloud recordings, and instant messages, files, whiteboards, and shared while using the service**."[50] Under a heading entitled "More about meeting recordings" the policy states: "If you participate in a Recorded Meeting or you subscribe to Zoom cloud recording services, we collect information from you in connection with and through such Recordings. This information may include Personal Data."[51]

119. As of April 2, 2020, Zoom "removed the attendee attention tracker feature as part of our commitment to the security and privacy of our customers."[52] Prior to its removal, this surreptitious tracking feature gave presenters the ability to "track if participants . . . clicked away from the active Zoom window for more than half a minute."[53]

120. Consumer Reports has pointed out that Zoom provides meeting hosts with the ability "make a recording of the conference, have it transcribed automatically, and share the information with people who aren't at the meeting."[54] Under Zoom's privacy policy, Zoom collects those video recordings and transcripts, as well as documents shared on the screen, and the name of everyone on a call.[55] Like other tech giants with access to large

---

[49] Zoom Privacy Policy (February 23, 2020) accessed via the Internet Archive Wayback Machine, available at <https://web.archive.org/web/20200311205042/https://zoom.us/privacy?zcid=1231> (Last Visited July 28, 2020) ("Zoom Privacy Policy (February 23, 2020)").

[50] *Id.*

[51] *Id.*

[52] <https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking> (last visited July 30, 2020); *see also* Eric S. Yuan, *A Message to Our Users* (April 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (Last Visited July 30, 2020).

[53] Karl Bode, *Working From Home? Zoom Tells Your Boss If You're Not Paying Attention*, available at <https://www.vice.com/en_us/article/qjdnmm/working-from-home-zoom-tells-your-boss-if-youre-not-paying-attention> (Last Visited July 30, 2020).

[54] Allen St. John, *Zoom Calls Aren't as Private as You May Think*, CONSUMER REPORTS (March 30, 2020), available at <https://www.consumerreports.org/video-conferencing-services/zoom-teleconferencing-privacy-concerns/> (Last Visited July 29, 2020).

[55] *See id.*

troves of live video recordings, Zoom has incredible incentive to access and view that video and audio content.[56]

121. There are reports of Zoom sending presenters meeting transcripts that include transcriptions of supposedly private chats conducted between meeting participants, sometimes without the presenter's participation, and sometimes including embarrassing, personal content that those participating in the chats surely would not have included had they known the chats would be recorded.[57]

122. Such video conference recordings are extremely helpful in the development of highly capable artificial intelligence ("AI"). AI systems are highly valuable to businesses because they automate away the need for human workers. Virtual assistants or "chatbots" are one example of an AI that has immense monetary value. One firm estimated that the chatbot market was valued at USD 17.17 billion in 2019 and is projected to reach 102.29 billion by 2025.[58] "A chatbot is basically an artificial intelligence-powered application that converses with a human being to solve a problem or to answer a certain query... According to Salesforce, 69% of consumers prefer to use chatbots for the speed at which they can communicate with a brand. [59]

123. The catch: to build an effective AI model, companies need vast amounts of data. The more data, the better and more "human-like" the AI.[60] OpenAI recently released

---

[56] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), available at <https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP> (Last Visited July 29, 2020).

[57] *See, e.g.*, Danny M. Lavery, *I Saw My Co-Workers' Private DMs Mocking My Weight*, SLATE (April 25, 2020), available at <https://slate.com/human-interest/2020/04/dear-prudence-coworkers-private-dm-zoom-mocking-weight.html> (Last Visited July 30, 2020).

[58] *See* <https://www.mordorintelligence.com/industry-reports/chatbot-market> (Last Visited July 29, 2020).

[59] *Id.*

[60] Karen Hao, Facebook Claims Its New Chatbot Beats Google's As The Best In The World (April 29, 2020), available at <https://www.technologyreview.com/2020/04/29/1000795/facebook-ai-chatbot-blender-beats-google-meena/> (Last Visited July 29, 2020); Chris Knight, *How Much Data Do You Need To*

GPT-3, currently a language AI so advanced, that it was able to code basic HTML script to produce a simple website:

> Others have found that GPT-3 can generate any kind of text, including guitar tabs or computer code. For example, by tweaking GPT-3 so that it produced HTML rather than natural language, web developer Sharif Shameem showed that he could make it create web-page layouts by giving it prompts like "a button that looks like a watermelon" or "large text in red that says WELCOME TO MY NEWSLETTER and a blue button that says Subscribe." Even legendary coder John Carmack, who pioneered 3D computer graphics in early video games like Doom and is now consulting CTO at Oculus VR, was unnerved: "The recent, almost accidental, discovery that GPT-3 can sort of write code does generate a slight shiver."[61]

124. The key to effective AI models is access to large data sets. Indeed, MIT Technology Review points out that GPT-3 "is the largest language model ever created."[62] "The model has 175 billion parameters (the values that a neural network tries to optimize during training), compared with GPT-2's already vast 1.5 billion. And with language models, size really does matter."[63] For example, Google used 341GB of social media conversation data to train its chatbot "Meena," which has only 2.6 billion parameters.[64]

125. "The requirement for upgrading AI systems is more and more data, and more

---

Train A Chatbot and Where To Find It?, available at <https://chatbotslife.com/how-much-data-do-you-need-to-train-a-chatbot-and-where-to-find-it-d25a7b930e> (Last Visited July 29, 2020).

[61] Will Douglas Heaven, *OpenAI's New Language Generator GPT-3 Is Shockingly Good—And Completely Mindless,* MIT Technology Review (July 20, 2020), https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/ (Last Visited July 29, 2020).

[62] *Id.*

[63] *Id.*

[64] Daniel Adiwardana et al., Towards a Human-like Open-Domain Chatbot, available at <https://arxiv.org/pdf/2001.09977.pdf> (Last Visited July 29, 2020); Chris Knight, *How Much Data Do You Need To Train A Chatbot and Where To Find It?*, available at <https://chatbotslife.com/how-much-data-do-you-need-to-train-a-chatbot-and-where-to-find-it-d25a7b930e> (Last Visited July 29, 2020).

and more diverse data," according to Anil Jain, a professor at Michigan State University.[65] Zoom has access to the authentic and unscripted dialogue of millions of humans around the world, speaking in various languages, on diverse topics, with various levels of intimacy and formality—a veritable goldmine. A chatbot trained on transcripts of conversation between travel agents can be used to answer the questions of consumers who visit a travel website. A chatbot trained on conversations between students and teachers can become a more natural language sounding teaching tool.

126. The problem: training AI using Zoom's recorded content would invade the privacy of Zoom users. To train AI systems, according to Professor Jain, "human workers have to manually review and annotate recordings or other information. There's always a human touch involved at some point."[66] And not just humans—the AI itself will read the consumer data while being trained, and can be prompted to share that private consumer information with others. A collaboration between researchers at Google Brain, Berkeley, and the University of Singapore showed that the AI can spit back the personally identifiable information of a single data point which was intentionally placed in a large database:

> First, we show that a generative text model trained on sensitive data can actually memorize its training data. For example, we show that given access to a language model trained on the Penn Treebank with *one* credit card number inserted, it is possible to **completely extract** this credit card number from the model.[67]

[65] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP (Last Visited July 29, 2020).

[66] Thomas Germain and Daniel Wroclawski, *Do Tech Companies Watch Your Home Security Camera Footage?*, Consumer Reports (October 22, 2019), https://www.consumerreports.org/home-security-cameras/do-tech-companies-watch-your-home-security-camera-footage/?EXTKEY=AFLIP (Last Visited July 29, 2020).

[67] Nicholas Carlini, *Evaluating and Testing Unintended Memorization in Neural Networks* (Aug. 13, 2019), available at <https://bair.berkeley.edu/blog/2019/08/13/memorization/> (Last Visited July 29, 2020);

127. Both the audio and visual content of zoom users' recordings are extremely valuable in the creation of AI, and Zoom may be accessing and viewing consumers' video recordings without the users' consent or knowledge for such purposes.[68]

Misrepresentations Regarding End-to-End Encryption

128. End-to-end encryption ("E2E") is a system of communication where only the communicating users can read the messages.

129. Increasingly, E2E encryption is becoming an industry standard expectation for communication technology. Facebook announced in March 2019 that it would move all three of its messaging platforms (including WhatsApp) to E2E encryption. Similarly, Apple says of its data security: "iCloud is built with industry-standard security technologies, employs strict policies to protect your information, and is leading the industry by adopting privacy-preserving technologies like end-to-end encryption for your data."

130. Competitor platforms Webex and GoToMeeting both either automatically utilize E2E encryption or offer hosts the option of E2E encryption as part of their standard platform.

131. As a result, Zoom is and has been aware that E2E encryption is a valuable service that consumers will both pay for and have increasingly come to expect as part of their online communication choices.

132. With this in mind, Zoom has explicitly represented that it had E2E encryption functionality at least as early as 2019. For example, Zoom made representations that it "exceeds a high standard for data privacy and protection," "is certified and compliant with the EU-U.S. Privacy Shield Framework," as well as utilizing "end-to-end-encryption for

---

Nicholas Carlini, *The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks* (July 16, 2019), available at <https://arxiv.org/pdf/1802.08232.pdf> (Last Visited July 29, 2020).

[68] Blair Hanley Frank, *Zoom Uses AI to ADD Automatic Transcription to Its Videoconferencing Service* (Sept. 26, 2017), available at <https://venturebeat.com/2017/09/26/zoom-uses-ai-to-add-automatic-transcription-to-its-videoconferencing-service/> (Last Visited July 30, 2020); John Porter, *This Tool Automatically Transcribes Your Zoom Meetings as They Happen* (April 23, 2020), available at <https://www.theverge.com/2020/4/23/21232385/otter-ai-live-video-meeting-notes-zoom-transcription-annotation-teams> (Last Visited July 30, 2020).

desktop and mobile devices."[69]

133. Similarly, Zoom's own website prominently featured, on the "Security at Zoom" page, the statement that:

> We take security seriously and we are proud to exceed industry standards when it comes to your organization's communications
> . . . .
> The following in-meeting security capabilities are available to the meeting host:
> • Secure a meeting with end-to-end encryption
> . . .
> Zoom's solution and security architecture provides end-to-end encryption and meeting access controls so data in transit cannot be intercepted.[70]

134. Zoom also prominently linked to a "Security Whitepaper" on its "Security at Zoom" page which repeated these false claims regarding E2E encryption.[71]

135. Additionally, during Zoom videoconferences, hovering your cursor over the green lock at the top left corner of the application would show the text "Zoom is using an end to end encrypted connection." Zoom has since changed this text to simply say that the session is encrypted.

136. On March 31, 2020, The Intercept published an article revealing that Zoom video conferences, and Zoom's other audio and video functionality, did not in fact support E2E encryption.[72]

137. Zoom thereafter updated its encryption to the industry-standard AES-GCM with 256-bit keys. But the encryption keys for each meeting are generated by Zoom's

---

[69] *Zoom Executive Summary*, available at <https://www.neha.org/sites/default/files/Zoom%20Executive%20Summary%202019.pdf >, at 10 (Last Visited July 28, 2020).

[70] Security at Zoom, (March 22, 2020), accessed via the Internet Archive Wayback Machine, available at <http://web.archive.org/web/20200322145328/https://zoom.us/security> (Last Visited July 28, 2020).

[71] Zoom Security Guide, (March 31, 2020), accessed via the Internet Archive Wayback Machine, available at <http://web.archive.org/web/20200331082306/https://zoom.us/docs/doc/Zoom-Security-WhitePaper.pdf> (Last Visited July 28, 2020).

[72] Micah Lee and Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading* (March 31, 2020), <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (Last Visited July 28, 2020).

servers, not by the client devices. The connection between the Zoom app running on a user's computer or phone and Zoom's server is encrypted in the same way the connection between a web browser and a website is encrypted. This is known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. In a Zoom meeting utilizing this encryption technology, the video and audio content will stay private from anyone spying on Wi-Fi, but will not stay private from the company or, presumably, anyone with whom the company shares its access voluntarily, by compulsion of law (*e.g.*, at the request of law enforcement), or involuntarily (*e.g.*, a hacker who can infiltrate the company's systems). With true E2E encryption, the encryption keys are generated by the client (customer) devices, and only the participants in the meeting have the ability to decrypt it.[73]

138. Matthew Green, a cryptographer and computer science professor at Johns Hopkins University, points out that group video conferencing is difficult to encrypt end-to-end. That's because the service provider—in this case Zoom—needs to detect who is talking to act like a switchboard, in order to send a high-resolution videostream from the person who is talking at the moment, and low-resolution videostreams of other participants. This type of optimization is much easier if the service provider can see everything because it's unencrypted, but it is possible. Apple FaceTime, for example, utilizes E2E encryption.[74]

139. Zoom's own response on April 1, 2020 (the day after The Intercept's article) made it clear that Zoom both knew that it did not use the industry-accepted definition of E2E encryption and had made a conscious decision to use the term "end-to-end" anyway.[75]

140. This is particularly egregious in light of Zoom's representations regarding compliance with the Health Insurance Portability and Accountability Act ("HIPAA").

---

[73] *Id.*

[74] *Id.*

[75] Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars* (Apr. 1, 2020), available at <https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/> (Last Visited July 28, 2020).

Zoom has encouraged patients and health care professionals to use its videoconferencing services for private and sensitive medical appointments.[76] Any person doing so would assume that no-one but the doctor and patient were capable of viewing such a conversation. As is apparent from the above explanation, however, Zoom itself (and anyone who knowingly or unknowingly gained access to Zoom's system) can view those videoconferences.

"Zoombombing"

141. Further failures of Zoom's security procedures have arisen with a troubling phenomenon referred to as "Zoombombing." Zoombombing involves unauthorized participants entering Zoom meetings to disrupt them with offensive behavior such as posting racial slurs and other derogatory statements. Following the issuance of local and state stay-at-home orders, schools, churches, synagogues, mosques, support groups, and medical providers have all moved their meetings online using Zoom's video conferencing service to connect students, teachers, parishioners, participants and patients.

142. Just as schools, businesses, support groups, and religious institutions and millions of individuals have adopted Zoom as a meeting platform in an increasingly remote world, reports of Zoombombing by uninvited participants have become frequent.[77]

143. On April 3, 2020, the New York Times reported that "While those incidents may have initially been regarded as pranks or trolling, they have since risen to the level of hate speech and harassment, and even commanded the attention of the F.B.I."[78]

144. An analysis by The New York Times found "153 Instagram accounts, dozens of Twitter accounts and private chats, and several active message boards on Reddit and

[76] *See, e.g.*, Zoom, *HIPAA Compliance Guide*, available at <https://zoom.us/docs/doc/Zoom-hipaa.pdf> (Last Visited July 28, 2020); <https://marketplace.zoom.us/apps?category=health_care> (describing healthcare app partners) (Last Visited July 28, 2020).

[77] Taylor Lorenz and Davey Alba, *'Zoombombing' Becomes a Dangerous Organized Effort,* New York Times (April 3, 2020), available at <https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html> (Last Visited July 28, 2020).

[78] *Id.*

4Chan where thousands of people had gathered to organize Zoom harassment campaigns, sharing meeting passwords and plans for sowing chaos in public and private meetings."[79]

145. As early as March 20, 2020, Zoom admitted its product had an issue with Zoombombing.[80] Rather than change security protocols and default features, however, Zoom turned its back on its users, asserting they were to blame through their inability to properly use the program.

146. Nevertheless, reports of Zoombombings with bad actors displaying pornography, screaming racial epitaphs, or engaging in similarly despicable conduct have continued to the present day. Bad actors have disrupted private moments as diverse as Alcoholics Anonymous meetings to Holocaust memorial services (in one instance by displaying images of Adolf Hitler).[81] School classes and religious services all over the world have been affected. Recordings of these incidents and others end up on YouTube and TikTok with the horrified reactions of participants being the digital trophies of the Zoombombers.[82] Concerns regarding Zoombombing led many organizations to ban employee use, including Google, SpaceX, NASA, the Australian Defence Force, the Taiwanese and Canadian governments, the New York Department of Education, and the Clark County School District in Nevada.[83]

147. The Zoombombing incidents experienced by Saint Paulus and Oak Life Church and their church members were consistent with those experienced by others across the country. Both incidents involved disturbing display of child pornography images and video to participants during regularly-scheduled church services. Both incidents involved

---

[79] *Id.*

[80] *How to Keep Uninvited Guests Out of Your Zoom Event* (March 20, 2020), available at <https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/> (Last Visited July 28, 2020).

[81] Sebastien Meineck, *'Zoom Bombers' Are Still Blasting Private Meetings With Disturbing and Graphic Content* (June 10, 2020), available at <https://www.vice.com/en_us/article/m7je5y/zoom-bombers-private-calls-disturbing-content> (Last Visited July 28, 2020).

[82] *Id.*

[83] *Id.*

offenders that were "known" to Zoom but as to whom Zoom failed to take any action. Both incidents caused irreparable harm to already-vulnerable communities, requiring trauma counselling and emotional support groups in case of Oak Life Church, and were so severe as to require them to be reported to law enforcement, including the FBI.

148. Given these incidents, Zoom's representations that it "takes its users' privacy extremely seriously" and that its "customers' privacy is incredibly important to" it cannot be taken at face value. To date Zoom has marketed itself to institutions and to the pubic under the false premise that its Zoom meetings are secure. If they were secure, Zoom participants would not be subjected to racial slurs and other abusive behavior by Zoombombers.

149. Had Zoom informed its users that it would not engage in a thorough review of its security protocols, or that it would create default settings or other security holes that could be exploited by malicious actors, customers—like Plaintiffs and Class members—would not have been willing to purchase its services at the price charged, or even to use those services at all, regardless of price.

150. Zoom's failure to implement adequate security protocols jeopardized millions of consumers' privacy, fell well short of its promises, and diminished the value of the products and services provided. In other words, because Defendant failed to disclose its gross security inadequacies, and exposed users to malicious third parties' harassment, without their informed consent, it delivered fundamentally less useful and less valuable products and services than those for which consumers like Plaintiffs paid and/or expected when they chose to use Zoom's services.

151. While Zoom's wrongful conduct constitutes invasion of privacy in and of itself, entitling consumers to damages, Plaintiffs and Class members are also now placed at an increased risk of further imminent harm as a direct result of Zoom's wrongful acts and omissions.

THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT RULE

152. Congress enacted the Children's Online Privacy and Protection Act

("COPPA") in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information online by operators of Internet Web sites and online services. COPPA directed the Federal Trade Commission to promulgate a rule implementing COPPA, 16 C.F.R. Part 312 ("COPPA Rule").

153. The COPPA Rule applies to any operator of a commercial Web site or online service directed to children that collects, uses, and/or discloses personal information from children, or on whose behalf such information is collected or maintained, and to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. Defendant Zoom specifically advertises its video conferencing service to schools and children.

154. The COPPA Rule defines "personal information" to include, among other things, a first and last name; a home or other physical address including street name and name of a city or town; online contact information (*i.e.*, an email address or other substantially similar identifier that permits direct contact with a person online, such as an instant messaging user identifiers, screen name, or user name); a persistent identifier such as an IP address that can be used to recognize a user over time and across different Web sites or online services; a photograph, video, or audio file where such file contains a child's image or voice; or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. Through its video conferencing services, Defendant collected personal information as defined in the COPPA Rule, including children's names, addresses, IP addresses, and photographs and audio files containing a child's image or voice. Defendant also collected information from the child concerning the child that was combined with other identifiers, such as the name or photograph of the child.

155. Because Defendant collects and maintains personal information from its users through its video conferencing services, Defendant is an operator as defined by the COPPA Rule, 16 C.F.R. § 312 *et seq.*.

156. Among other things, the Rule requires that an operator of a child-directed website or online service meet specific requirements prior to collecting online, using, or disclosing personal information from children, including but not limited to:

a. posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information it collects from children, how it uses such information, and its disclosure practices for such information, and other specific disclosures set forth in the Rule;

b. providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents;

c. obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; and

d. establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

157. Defendant has failed to comply with each of these requirements as outlined in the failures and events described above, including but not limited to, Defendant's failure to properly post its privacy policy, failing to properly provide its information practices, failing to properly obtain parental consent, and failing to establish and maintain reasonable practices to protect personal information and prevent unauthorized access to video conferences.

CLASS ALLEGATIONS

158. Plaintiffs bring this class action lawsuit individually and on behalf of the proposed Class under Rule 23 of the Federal Rules of Civil Procedure.

159. Plaintiffs seek certification of a Nationwide Class and an Under 13 Sub-Class (collectively, the "Classes") defined as follows:

> Nationwide Class: All persons in the United States who used Zoom.

160. In the alternative, Plaintiffs seek certification of the following nationwide class of children under the age of 13:

Under 13 Sub-Class: All persons under the age of 13 in the United States who used Zoom.

161. Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

162. The Classes meet the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the following reasons.

163. **Numerosity:** Although the exact number of Class members is uncertain, and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable, believed to amount to many thousands or millions of persons. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and the Court. Information concerning the exact size of the putative class is within the possession of Defendant. The parties will be able to identify each member of the Classes after Defendant's document production and/or related discovery.

164. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant collected Plaintiffs' and Class members' personal data;

c. Whether Defendant provided Plaintiffs' personal data to third parties;

d. Whether Defendant adequately disclosed its policy of providing personal data to third parties;

e. Whether Defendant's collection and storage of Plaintiffs' and Class and members' personal data in the manner alleged violated federal, state and local laws, or industry standards;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by providing personal data to third parties;

g. Whether Defendant violated the consumer protection and privacy statutes applicable to Plaintiffs and members of the Class;

h. Whether Defendant acted negligently in failing to properly safeguard Plaintiffs' and Class members' personal data;

i. Whether Defendant's acts and practices complained of herein amount to egregious breaches of social norms; and

j. The nature of the relief, including equitable relief, to which Plaintiffs and Class members are entitled.

165. **Typicality:** Plaintiffs' claims are typical of the claims of other Class members. Plaintiffs and other Class members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

166. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

167. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, Defendant's database still exists, and Defendant may still be intentionally or inadvertently providing data to third parties – one standard of conduct is needed to ensure the future handling of Defendant's database.

168. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

169. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class members in the proposed Classes.

170. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

171. **Certification of Particular Issues:** In the alternative, this action may be maintained as class action with respect to particular issues in accordance with Fed. R. Civ. P. 23(c)(4).

172. Finally, all members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for members of the Classes, which can be used to identify Class members.

FIRST CAUSE OF ACTION
Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(*On Behalf of Plaintiffs and all Classes*)

173. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

174. Plaintiffs and Class members have a legally protected privacy interest in their private and personal information that is transferred to or recorded by Zoom, and are entitled to the protection of their property and information against unauthorized access.

175. Plaintiffs and Class members reasonably expected that their personal data would be protected and secure from unauthorized parties, and that their private and

personal information would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

176. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class members by (a) failing to adequately secure their private and personal information from disclosure to unauthorized parties for improper purposes; (b) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiffs and Class members, including but not limited to Zoom's unauthorized sharing of personal information with Facebook, Zoom's data-mining related to its LinkedIn plug-in, Zoom's failure to implement E2E encryption, and Zoom's failure to secure users' meetings against Zoombombings. This invasion into the privacy interest of Plaintiffs and Class members is serious and substantial.

177. In failing to adequately secure Plaintiffs' and Class members' personal information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its substandard security measures would cause its users harm and, would be considered highly offensive to a reasonable person in the same position as Plaintiffs and Class members.

178. Defendant violated Plaintiffs' and Class members' right to privacy under California law, including, but not limited to, Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

179. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and Class members' private, personal, and confidential information has been accessed or is at imminent risk of being accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and proposed Class members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

180. Plaintiffs and Class members are entitled to injunctive relief as well as actual

and punitive damages.

SECOND CAUSE OF ACTION
Negligence
(*On Behalf of Plaintiffs and all Classes*)

181. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

182. Defendant marketed and offered Zoom meetings to Plaintiffs and Class members with full knowledge of the purposes for which Zoom meetings were being used, as well as the highly sensitive nature of the information Zoom meetings involve.

183. Defendant owed a duty to Plaintiffs and Class members arising from the sensitivity of Plaintiffs' and Class members' information, and the privacy rights Zoom meetings were supposed to secure and protect, to exercise reasonable care in safeguarding such information and privacy rights. Defendant's duties included, among other things, the duty to design, maintain, implement, monitor, test, and comply with reliable security systems, protocols, and practices to ensure that Plaintiffs' and Class members' Zoom meetings were adequately secured from unauthorized access, and the duty to maintain the confidentiality of its users' private and personal information, including by refraining from sharing such information with unauthorized parties without users' informed and clear consent.

184. Defendant breached its duties by, among other things, (1) failing to implement and maintain reasonable security protections and protocols, including by implementing E2E encryption, in accordance with its representations, and sufficient security protocols to prevent Zoombombings; and (2) knowingly sharing and/or selling customers' personal data to third parties for analytics and marketing purposes without adequate disclosure to and consent from its customers, including Facebook and LinkedIn Sales Navigator subscribers.

185. Defendant's misconduct is inconsistent with industry regulations and standards.

186. But for Defendant's breaches of its duties, Plaintiffs' and Class members' Zoom meetings would have been protected from unauthorized access, and Plaintiffs' and

Class members' private and personal information would not have been compromised or obtained by third parties without consent.

187. Plaintiffs and Class members were foreseeable victims of Defendant's wrongful conduct complained of herein. Defendant knew or should have known that its failure to implement reasonable protocols to adequately secure its customers' Zoom meetings and restrict third-party access to customers' personal data would cause damages to Plaintiffs and Class members.

188. As a result of Defendant's negligent and/or willful failures, Plaintiffs and Class members suffered injury, which includes but is not limited to unauthorized offensive interruption of their most private conversations and resulting emotional distress, unauthorized release of private and personal data to third parties, exposure to a heightened, imminent risk of unauthorized access to their private and personal data and conversations, fraud, theft, and other financial harm. Plaintiffs and Class members must now more closely protect their private and personal data. The unauthorized access to Plaintiffs' and Class members' private and personal data also has diminished the value of that information.

189. The damages to Plaintiffs and Class members were a proximate, reasonably foreseeable result of Defendant's breaches of its duties.

190. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(*On Behalf of Plaintiffs and all Classes*)

191. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

192. Defendant provided Zoom meetings to Plaintiffs and members of the Class. In exchange, Defendant received benefits in the form of monetary payments and/or other valuable consideration, *e.g.*, access to their private and personal data.

193. Defendant has acknowledged these benefits and accepted or retained them.

194. In using Zoom meetings, Plaintiffs and Class members continually provide

Defendant with their private and personal information.

195. By providing that information, and upon Defendant's acceptance of that information, Plaintiffs and Class members, on the one hand, and Defendant, on the other, entered into implied contracts whereby Defendant agreed to and was obligated to take reasonable steps to secure and safeguard that sensitive information. Such safeguarding was integral and essential to Defendant's entire line of business, secure video conferencing services.

196. Under those implied contracts, Defendant was obligated to provide Plaintiffs and Class members with Zoom meetings that were suitable for their intended purpose of providing secure video conferencing services, rather than other video conferencing services vulnerable to unauthorized access, incapable of providing safety and security, and instead actually utilized to track its users' personal data for commercial purposes.

197. Without such implied contracts, Plaintiffs and Class members would not have used Zoom meetings and would not have conferred benefits on Defendant, but rather chosen alternative video conferencing services that did not present these privacy and safety risks.

198. Plaintiffs and Class members fully performed their obligations under these implied contracts.

199. As described throughout, Defendant did not take reasonable steps to safeguard Plaintiffs' and Class members' private information. In fact, Defendant willfully violated those privacy interests by tracking and disclosing its customers' personal data to third parties without consent.

200. Because Defendant failed to take reasonable steps to safeguard Plaintiffs' private information, Defendant breached its implied contracts with Plaintiffs and Class members.

201. Defendant's failure to fulfill its obligation to safeguard Plaintiffs' and Class members' private information resulted in Plaintiffs and Class members receiving video conferencing services that were of less value than they provided consideration for (*i.e.*,

unsecure video conferencing services without adequate security).

202. Stated otherwise, because Plaintiffs and Class members provided valuable consideration for secure video conferences and privacy protections they did not receive—even though such protections were a material part, if not the very essence, of their contracts with Defendant—the full benefit of their bargain.

203. As a result of Defendant's conduct, Plaintiffs and members of the Class have suffered actual damages in an amount equal to the difference in the value of the video conferencing services they provided valuable consideration for and the unsecure video conferences they received.

204. Accordingly, Plaintiffs, on behalf of themselves and Class members, seeks an order declaring that Defendant's conduct constitutes breach of implied contract, and awarding them damages in an amount to be determined at trial.

FOURTH CAUSE OF ACTION
Breach of Implied Covenant of Good Faith and Fair Dealing
(*On Behalf of Plaintiffs and all Classes*)

205. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

206. There is a covenant of good faith and fair dealing implied in every implied contract. This implied covenant requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement. To fulfill its covenant, a party must give at least as much consideration to the interests of the other party as it gives to its own interests.

207. Under the implied covenant of good faith and fair dealing, Zoom is obligated to, at a minimum, (a) implement proper procedures to safeguard the personal information of Plaintiffs and other Class members; (b) refrain from disclosing, without authorization or consent, the personal information of Plaintiffs and other Class members to any third parties; (c) promptly and accurately notify Plaintiffs and other Class members of any unauthorized disclosure of, access to, and use of their personal information; and (d) maintain adequate security and proper encryption in Zoom's videoconferences.

208. Zoom breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook and LinkedIn Sales Navigator subscribers;
- allowing third parties to access the personal information of Plaintiffs and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

209. As a direct and proximate result of Zoom's breaches of the implied covenant of good faith and fair dealing, Plaintiffs and other Class members have suffered actual losses and damages.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(*On Behalf of Plaintiffs and all Classes*)

210. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

211. Defendant received a benefit from Plaintiffs and Class members in the form of payments and/or other valuable consideration including access to their private and personal data, in exchange for videoconferencing services.

212. Those benefits received by Defendant were at the expense of Plaintiffs and Class members.

213. The circumstances alleged herein are such that it would be unjust for Defendant to retain the portion (if not the entirety) of Plaintiffs' and Class members' payments, or the value of other consideration, that should have been earmarked to provide

secure and reliable videoconferencing services, and adequate privacy and security procedures and safeguards for Plaintiffs' and the Class' private information, including only third-party sharing as authorized by its customers.

214. Plaintiffs seek an order directing Zoom to disgorge these benefits and profits and pay restitution to Plaintiffs and other Class members.

SIXTH CAUSE OF ACTION
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*
(*On Behalf of Plaintiffs and all Classes*)

215. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

216. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

217. Defendant engaged in unfair, fraudulent, and unlawful business practices in connection with its provision of Zoom meetings, in violation of the UCL.

218. As alleged herein, Defendant expressly represented to consumers such as Plaintiffs and Class members, among other things: that Zoom meetings were secure, including by use of E2E encryption; and that Defendant would maintain adequate security practices and procedures to protect Plaintiffs' and Class members' private information from unauthorized access. Defendant also omitted or concealed the material fact of its inadequate privacy and security measures, and thus failed to disclose to Plaintiffs and Class members that it failed to meet legal and industry standards for the protection of Zoom meetings and consequently, its customers' private property and information. Defendant also concealed its commercial tracking and sharing of customers' personal data with third parties.

219. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

220. Defendant violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiffs' and Class members' constitutional rights to privacy, state and federal privacy

statutes, and state consumer protection statutes, such as The Children's Online Privacy Protection Act, 16 C.F.R. § 312.5 ("COPPA"), The Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 ("CalOPPA"), the California Invasion of Privacy Act ("CIPA"), and The Health Insurance Portability and Accountability Act ("HIPAA").

221. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Class members. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

222. By exposing, compromising, and willfully sharing and/or selling Plaintiffs' and Class members' private property and personal information without authorization, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

223. A reasonable person would not have agreed to purchase and/or use Zoom meetings software and services had he or she known the truth about Defendant's practices alleged herein. By withholding material information about its practices, Defendant was able to convince customers to use Zoom meetings and to entrust their highly personal information to Defendant. Accordingly, Defendant's conduct also was "fraudulent" within the meaning of the UCL.

224. As a result of Defendant's violations of the UCL, Plaintiffs and Class members are entitled to injunctive relief.

225. As a result of Defendant's violations of the UCL, Plaintiffs and Class members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration, e.g. access to their private and personal data. The unauthorized access to Plaintiffs' and Class members' private and

personal data also has diminished the value of that information.

226. In the alternative to those claims seeking remedies at law, Plaintiffs and Class members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful, unfair, and fraudulent practices. Further, no legal remedy exists under COPPA, CalOPPA, and HIPAA. Therefore, Plaintiffs and members of the proposed Class are entitled to equitable relief to restore Plaintiffs and Class members to the position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct, restitution, and disgorgement of all profits paid to Defendant as a result of its unfair, deceptive, and fraudulent practices.

SEVENTH CAUSE OF ACTION
Violation of the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*
(*On Behalf of Plaintiffs and all Classes*)

227. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

228. California's Consumers Legal Remedies Act ("CLRA") has adopted a comprehensive statutory scheme prohibiting various deceptive practices in connection with the conduct of a business providing goods, property, or services to consumers primarily for personal, family, or household purposes. The self-declared purposes of the CLRA are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

229. Defendant is a "person" as defined by Civil Code Section 1761(c), because it is a corporation, as set forth above.

230. Plaintiffs and Class members are "consumers" within the meaning of Civil Code Section 1761(d).

231. Zoom meeting software purchased by Plaintiffs and the Class constitute "goods" and within the meaning of Cal. Civ. Code § 1761(a).

232. Zoom meeting services purchased by Plaintiffs and the Class constitute "services" within the meaning of Cal. Civ. Code § 1761(b).

233. Defendant's sale of Zoom meeting software to Plaintiffs and the Class constitute "transactions," as defined by Cal. Civ. Code § 1761(e).

234. Plaintiffs and Class members purchased Zoom meetings software and services from Defendant stores for personal, family, and household purposes, as defined by Cal. Civ. Code § 1761(d).

235. Venue is proper under Cal. Civ. Code § 1780(d) because a substantial portion of the conduct at issue occurred in this District. An affidavit establishing that this Court is the proper venue for this action is attached below.

236. As described herein, Defendant's practices constitute violations of California Civil Code Section 1770 in at least the following respects:

a. In violation of Section 1770(a)(5), Defendant misrepresented that Zoom meeting software and services had characteristics, benefits, or uses that they do not have (being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

b. In violation of Section 1770(a)(7), Defendant misrepresented that Zoom meeting software and services were of a particular standard, quality, and/or grade when they were of another (being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

c. In violation of Section 1770(a)(9), Defendant advertised Zoom meeting software and services with an intent not to sell them as advertised (advertising them as being E2E encrypted and private and secure from unauthorized third-party access when in fact they are not);

d. In violation of Section 1770(a)(16), Defendant misrepresented that Zoom meeting software and services were supplied in accordance with previous representations when they were not (that they are E2E encrypted and private and secure from unauthorized third-party access when in fact they are not).

237. Defendant's misrepresentations regarding Zoom meeting software and services were material to Plaintiffs and Class members because a reasonable person would

have considered them important in deciding whether or not to purchase Zoom meeting software and services.

238. Plaintiffs and Class members relied upon Defendant's material misrepresentations and would have acted differently had they known the truth.

239. As a direct and proximate result of Defendant's material misrepresentations, Plaintiffs and Class members have been irreparably harmed.

240. In accordance with Cal. Civ. Code § 1782(a), prior to the filing of this Complaint, Plaintiffs' counsel served Defendant with notice of these CLRA violations by certified mail, return receipt requested. Defendant has responded and refused agree to rectify the violations detailed above and give notice to all affected consumers.

241. On behalf of Class members, Plaintiffs seek injunctive relief in the form of an order enjoining Defendant from making such material misrepresentations and to engage in a corrective advertising to alert consumers of these misrepresentations.

242. Since Defendant refused to agree to rectify the violations detailed above and give notice to all affected consumers within 30 days of the date of written notice, Plaintiffs also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CLRA violations.

EIGHTH CAUSE OF ACTION
Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"),
Cal. Penal Code § 502
(*On Behalf of Plaintiffs and all Classes*)

243. Plaintiffs incorporate the foregoing allegations as if fully set forth here.

244. The California Legislature enacted the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") to "expand the degree of protection afforded. . . from tampering, interference, damage, and unauthorized access to (including the extraction of data from) lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and

computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals. . . ." Cal. Penal Code § 502(a).

245. Plaintiffs' devices on which they participated in Zoom videoconferences, including their computers, smart phones, and tablets constitute "computers, computer systems, and/or computer networks" within the meaning of the CDAFA.

246. Defendant violated § 502(c)(1)(B) of the CDAFA by knowingly accessing and without permission accessing Plaintiffs' and Class members' devices in order to obtain their personal information, including their device and location data, and in order for Defendant to share that data with third parties including Facebook and LinkedIn Sales Navigator Subscribers, in violation of Zoom users' reasonable expectations of privacy in their devices and data.

247. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information.

248. The computers and mobile devices that Plaintiffs and Class members used to participate in Defendant's videoconferences all have and operate "computer services" within the meaning of the CDAFA. Defendant violated §§ 502(c)(3) and (7) of the CDAFA by knowingly and without permission accessing and using those devices and computer services, or causing them to be accessed and used, *inter alia* in connection with Defendant's sharing of information with third parties including Facebook, Google, and in some cases other users of Defendant's videoconferencing services who were able to access user data through, for example the LinkedIn Sales Navigator app.

249. Defendant violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly and without permission providing and/or assisting in providing third parties, including, but not limited to, Facebook, Google, and LinkedIn Sales Navigator Subscribers, a means of accessing Plaintiffs' and Class members' computers and mobile devices.

250. Under California Penal Code § 502(b)(10) a "Computer contaminant" is

defined as "any set of computer instructions that are designed to ... record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

251. Defendant violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the Class Members and websites; including but not limited to the code that intercepted Plaintiffs' and the Class Members' private and personal data during Zoom meetings and transmitted that data to Facebook, Google, and to LinkedIn Sales Navigator subscribers.

252. As a direct and proximate result of Defendant's unlawful conduct within the meaning of California Penal Code § 502, Defendant caused loss to Plaintiffs and the Class Members in an amount to be proven at trial, including that Plaintiffs and the Class Members were injured by the loss of value of their personal information. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees under California Penal Code § 502(e)(2).

253. Plaintiffs and the Class Members seek compensatory damages in accordance with California Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

254. Plaintiff and Class Members have suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendant is enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

255. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

256. Plaintiffs and the Class Members have also suffered irreparable injury from these unauthorized acts of disclosure: their personal, private, and sensitive communications

have been harvested, viewed, accessed, stored, and used by Defendant, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitling Plaintiffs to injunctive relief.

NINTH CAUSE OF ACTION
Deceit by Concealment, Cal. Civ. Code § 1710(3)
(*On Behalf of Plaintiffs and all Classes*)

257. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

258. As detailed above, Zoom failed to disclose and actively concealed information about flaws that undermined the security and privacy of Zoom Meetings, including with respect to encryption levels. As Zoom knew, its knowledge was exclusive to the company and was not generally known to the public or to Zoom users, and had a duty to disclose the fact to Plaintiffs and Class members.

259. Zoom knew that the privacy and security of its videoconferencing service was materially worse than it represented and what Plaintiffs and Class members reasonably expected and intentionally concealed or suppressed the fact with intent to defraud Plaintiffs and Class members.

260. The information Zoom concealed was material in that it was important to reasonable persons, and Plaintiffs and Class members would not have acted as they did if they had known of the concealed or suppressed fact. As a result, Plaintiffs and Class members purchased Zoom Meetings they would not otherwise have purchased or paid significantly more for Zoom Meetings than they otherwise would have. Furthermore, had Plaintiffs known of the inadequate privacy and security of Zoom's videoconferencing services, Plaintiffs would have taken steps to protect themselves and/or their personal information.

261. Additionally, Plaintiffs and Class members would have taken the appropriate steps to protect themselves had they known Zoom had inadequate security.

262. Plaintiffs seek an award of all available damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter a judgment in his favor and against Defendant, as follows:

A. Determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure and appointing and his Counsel to represent the Class;

B. Finding Defendant's conduct was unlawful as alleged herein;

C. Enjoining Defendant from engaging in the wrongful conduct complained of herein;

D. Requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Awarding Plaintiffs and Class members actual damages, compensatory damages, punitive damages, statutory damages, and statutory penalties, in an amount to be determined;

F. Awarding Plaintiffs and Class members costs of suit and attorneys' fees, as allowable by law; and

G. Granting such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated: July 30, 2020

/s/ Tina Wolfson

Tina Wolfson
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111; Fax: (310) 474-8585

/s/ Mark C. Molumphy
Mark C. Molumphy
mmolumphy@cpmlegal.com
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577

Interim Co-Lead Counsel for Plaintiffs

Rachele R. Byrd
byrd@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Symphony Towers
750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
Fax: (619) 234-4599

Albert Y. Chang
achang@bottinilaw.com
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Avenue, Suite 102
La Jolla, CA 92037
Tel: (858) 914-2001
Fax: (858) 914-2002

Eric H. Gibbs
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Telephone: (510) 350-9700
Fax: (510) 350-9701
ehg@classlawgroup.com

Plaintiffs' Steering Committee

AFFIDAVIT OF TINA WOLFSON

I, Tina Wolfson, declare as follows:

1. I am an attorney with the law firm of Ahdoot & Wolfson, PC, counsel for Plaintiffs in this action. I am admitted to practice law in California and before this Court, and am a member in good standing of the State Bar of California. This declaration is made pursuant to California Civil Code section 1780(d). I make this declaration based on my research of public records and upon personal knowledge and, if called upon to do so, could and would testify competently thereto.

2. Venue is proper in this Court because many of the acts and transactions giving rise to this action occurred in this District, and Defendant (1) is authorized and registered to conduct business in this District, (2) has intentionally availed itself of the laws and markets of this District through the distribution and sale of its merchandise in this District, and (3) is subject to personal jurisdiction in this District.

3. Plaintiff Heddi Cundle is a resident of California.

4. Plaintiff M.F. is a resident of California.

5. Plaintiff Isabelle Gmerek is a resident of California.

6. Plaintiff Therese Jimenez is a resident of California.

7. Plaintiff Lisa Johnston is a resident of California.

8. Plaintiff Saint Paulus Lutheran Church is a citizen of the State of California.

9. Plaintiff Oak Life Church is a citizen of the State of California.

10. Defendant Zoom Video Communications, Inc. is a Delaware corporation with its principal place of business at 55 Almaden Blvd, San Jose, California 95113. Defendant is registered and authorized to conduct business and regularly conducts business in the State of California.

I declare under penalty of perjury under the laws of the United States and the State of California this 30th day of July, 2020 in Los Angeles, California that the foregoing is true and correct.

/s/ Tina Wolfson
Tina Wolfson